

# On the Automorphism Groups and Equivalence of Cyclic Combinatorial Objects

Kenza Guenda and T. Aaron Gulliver \*

## Abstract

We determine the permutation groups that arise as the automorphism groups of cyclic combinatorial objects. As special cases we classify the automorphism groups of cyclic codes. We also give the permutations by which two cyclic combinatorial objects on  $p^m$  elements are equivalent.

## 1 Introduction

Let  $n$  be a positive integer and  $S_n$  the group of permutations on  $n$  elements. A combinatorial object  $\mathcal{C}$  on  $n$  elements is called cyclic if its automorphism group  $Aut(\mathcal{C})$  contains the complete cycle  $T = (1, 2, \dots, n)$  of length  $n$ . Let  $C_p$  denote the cyclic group of order  $p$ .

The class of cyclic objects includes circulant graphs, circulant digraphs, cyclic designs and cyclic codes. Two cyclic combinatorial objects  $\mathcal{C}$  and  $\mathcal{C}'$  on  $n$  elements in the same category of objects are said to be equivalent if there exists a permutation  $\sigma$  of the symmetric group  $S_n$  acting on  $\{0, 1, \dots, n-1\}$  such that  $\mathcal{C}' = \sigma\mathcal{C}$ . When  $n$  is a prime number, it has been proven by Bays and Lambossey [4, 28] that circulant graphs are equivalent by a permutation  $\mu$  if and only if  $\mu$  satisfies  $\mu(i) = ai \pmod{n}$  for  $a \pmod{n}$  such that  $(a, n) = 1$ . Such permutations are called multipliers. Alspach and Parson [1] proved that two circulant graphs or digraphs on  $pq$  vertices, where  $p > q$  are two distinct primes, are equivalent if and only if they are equivalent by a multiplier. These results hold for all cyclic combinatorial objects in the case that  $Aut(\mathcal{C})$  has a  $p$ -Sylow subgroup of order  $p$  [1, Case 1]. Muzychuk [34] proved that this result also holds for circulant graphs in the square-free case. More generally, Palfy proved that if  $n$  is such that  $(n, \phi(n)) = 1$ , or  $n = 4$ , then two cyclic combinatorial objects are equivalent if and only if they are equivalent by a multiplier. Furthermore, Palfy gave a class of cyclic combinatorial objects on  $n$  elements where  $n \neq 4$  and  $\gcd(n, \phi(n)) \neq 1$  such that the class contains equivalent objects that are not equivalent by a multiplier.

---

\*T. Aaron Gulliver is with the Department of Electrical and Computer Engineering, University of Victoria, PO Box 3055, STN CSC, Victoria, BC, Canada V8W 3P6. email: agullive@ece.uvic.ca.

Brand [10] proved that cyclic combinatorial objects on  $p^m$  elements can be equivalent only under a specific set of permutations which depends on the  $p$ -Sylow subgroup of  $\text{Aut}(\mathcal{C})$ . Building on Brand's results [10], Huffman et al. [23] solved the equivalency problem for cyclic combinatorial objects and cyclic codes in the case  $n = p^2$ . This was achieved by explicitly determining the set of permutations under which two cyclic combinatorial objects or extended cyclic objects can be equivalent. In [23], a negative answer was given to the generalization of their results to the case  $n = p^m$ ,  $m > 2$ . This is due to the fact that the polynomials of Brand that are crucial to proving the results do not generate a Sylow subgroup of  $S_{p^m}$ . More recently, Babai et al. [2] gave an exponential time algorithm for determining the equivalence of two linear codes. In this paper, we consider the equivalency problem of cyclic combinatorial objects of length  $p^m$ . We generalize the results of [23] (which are only for the case  $n = p^2$ ), by explicitly giving the permutations by which two cyclic codes of length  $p^m$  are equivalent. This allows us to develop an algorithm which solves the equivalency problem by checking no more than  $\lceil \log_2(p-1) \rceil + 1$  permutations in the automorphism group. We also classify the automorphism groups of cyclic combinatorial objects. This requires knowledge of the  $p$ -Sylow subgroup of  $\text{Aut}(\mathcal{C})$ . We consider the special case of cyclic codes. Even though these codes are well known and have been studied extensively, very little is known about their automorphism groups, in particular the BCH and Reed-Solomon codes [5–7].

Beside the theoretical interest in automorphism groups and equivalence, there are many practical applications. Algorithms capable of determining graph equivalency can be used in optical character recognition [37] and image processing. Further, the automorphism groups and equivalency of cyclic codes can be employed in permutation decoding [8] and determining the weight distribution of a code [29]. While the equivalency of cyclic design find application in optical orthogonal codes [15]. The remainder of this paper is organized as follows. In Section 2, we investigate the automorphisms of cyclic objects. We also classify the automorphism groups of cyclic combinatorial objects. Section 3 considers the automorphism groups of cyclic codes. New results concerning the automorphism groups of cyclic codes of length  $p^m$  are presented. We also give an algorithm to find cyclic codes of length  $p$ . This algorithm requires that only  $p-1$  permutations be checked. In Section 4, we simplify and generalize some results of Huffman et al. [23] from length  $p^2$  to length  $p^m$ . This allows us to provide a solution to the equivalency problem for cyclic combinatorial objects. An algorithm to solve the equivalency problem is then presented which requires checking at most  $\lceil \log_2(p-1) \rceil + 1$  permutations.

Throughout this paper,  $\text{ord}_n(q)$  denotes the multiplicative order of  $q$  modulo  $n$ . In other words it is the smallest integer  $r$  such that  $q^r \equiv 1 \pmod{n}$ . The group  $\text{Aut}(\mathcal{C})$  denotes the automorphism group of the object  $\mathcal{C}$  (with elements which are permutations from  $S_n$ ). We denote by  $z$  the largest integer such that  $p^z \mid (q^{t'} - 1)$ , where  $t'$  is the order of  $q$  modulo  $p$ .

## 2 The Automorphism Groups of Cyclic Objects

We begin this section with some well known definitions. Let  $n$  be a positive integer. The set of permutations  $AG(n) = \{\tau_{a,b} : a \neq 0, (a, n) = 1, b \in \mathbb{Z}_n\}$  is the subgroup of  $S_n$  formed by the permutations defined as follows

$$\begin{aligned} \tau_{a,b} : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ x &\longmapsto (ax + b) \bmod n. \end{aligned} \tag{1}$$

The group  $AG(n)$  is called the group of affine transformations. The affine transformations  $M_a = \tau_{a,0}$  are also multipliers. The affine group  $AGL(1, p)$  is the group of affine transformations over  $\mathbb{Z}_p$ . The projective semi-linear group  $P\Gamma L(d, t)$  is the semi-direct product of the projective linear group  $PGL(d, t)$  and the automorphism group  $Z = Gal(\mathbb{F}_t/\mathbb{F}_p)$  of  $\mathbb{F}_t$ , where  $t = p^s$ ,  $p$  prime, i.e.

$$P\Gamma L(d, t) = PGL(d, t) \rtimes Z.$$

The orders of these groups are  $|PGL(d, t)| = (d, t-1)|PSL(d, t)|$ ,  $|Z| = s$  and  $|P\Gamma L(d, t)| = s|PGL(d, t)|$ .

**Remark 2.1** *If  $(d, t-1) = 1$ , then  $PGL(d, t) = PSL(d, t)$ . If  $t$  is a prime we have  $P\Gamma L(d, t) = PGL(d, t)$ .  $\square$*

From the fact that the automorphism group of a cyclic combinatorial object contains the complete cycle  $T$  of length  $n$ , we can easily prove that this group is transitive. A transitive group is either primitive or imprimitive. An interesting class of primitive groups is the class of doubly-transitive groups. A doubly-transitive group  $G$  has a unique minimal normal subgroup  $N$  which is either regular and elementary abelian or simple and primitive, and has centralizer  $C_G(N) = 1$  [13, p. 202]. All simple groups which can occur as a minimal normal subgroup of a doubly-transitive group are known. This result is due to the classification of finite simple groups. Using this classification, McSorley [31] gave the following result.

**Lemma 2.2** *A group  $G$  of degree  $n$  which is doubly-transitive and contains a complete cycle has socle  $N$  with  $N \leq G \leq Aut(N)$ , and is equal to one of the cases in Table 1.  $\square$*

As a direct application of Lemma 2.2, we obtain the following result.

**Theorem 2.3** *Let  $\mathcal{C}$  be a cyclic combinatorial objects on  $p$  elements. Then  $Aut(\mathcal{C})$  is a primitive group with socle  $S$ , and one of the following holds:*

- (i)  $Aut(\mathcal{C}) = S_n$  or  $Alt(n)$ .

Table 1: The Doubly Transitive Groups that Contain a Complete Cycle

$G$	$n$	$N$
$AGL(1, p)$	$p$	$C_p$
$S_4$	4	$C_2 \times C_2$
$S_n, n \geq 5$	$n$	$Alt(n)$
$Alt(n), n \text{ odd and } \geq 5$	$n$	$Alt(n)$
$PGL(d, t) \leq G \leq P\Gamma L(d, t)$ $(d, t) \neq (2, 2), (2, 3), (2, 4)$	$\frac{t^d - 1}{t - 1}$	$PSL(d, t)$
$PSL(2, 11)$	11	$PSL(2, 11)$
$M_{11}(\text{Mathieu})$	11	$M_{11}(\text{Mathieu})$
$M_{23}(\text{Mathieu})$	23	$M_{23}(\text{Mathieu})$

(ii)  $Aut(\mathcal{C})$  is a solvable group of order  $pm$  with  $m$  a divisor of  $p - 1$  and  $S = C_p \leq Aut(\mathcal{C}) \leq AGL(1, p)$ . Furthermore  $Aut(\mathcal{C})$  contains a normal  $p$ -Sylow group.

(iii)  $Aut(\mathcal{C}) = PSL(2, 11)$ ; of degree 11.

(iv)  $Aut(\mathcal{C}) = M_{11}$  or  $Aut(\mathcal{C}) = M_{23}$  of degree 11 or 23, respectively.

(v)  $S = PSL(d, r^{d^b})$  and  $PGL(d, r^{d^b}) \leq Aut(\mathcal{C}) \leq P\Gamma L(d, r^{d^b})$  where  $d \in \mathbb{N}$ ,  $d \geq 3$  is a prime number such that  $(d, r - 1) = 1$ , and  $p = (r^{d^{b+1}} - 1)/(r^{d^b} - 1)$ .

**Proof.** A transitive group of prime degree is a primitive group [35, p. 195]. As a consequence of a result of Burnside [19, Theorem 2], a transitive group of prime degree is either a subgroup of  $AGL(1, p)$  or a doubly-transitive group. Since the order of  $AGL(1, p)$  is  $p(p - 1)$ , the order of any subgroup is  $pm$  where  $m|(p - 1)$ . By Sylow's Theorem,  $Aut(\mathcal{C})$  contains a unique  $p$ -Sylow group, so it is a normal subgroup. By [17, Ex. 3.5.1]  $G$  is solvable. The remaining cases follow from Lemma 2.2. A number theory argument [18, Lemma 3.1] gives that in case (iv) if  $p$  is prime, then  $d$  must be a prime such that  $(d, r^a - 1) = 1$  and  $a = d^b$ . The result then follows.  $\square$

The following result is obtained by considering the automorphism groups of cyclic objects of composite length.

**Theorem 2.4** *Let  $\mathcal{C}$  be a cyclic combinatorial object on  $n$  elements such that  $n$  is a composite number. Then  $Aut(\mathcal{C})$  is either*

(i) *an imprimitive group (in the case that  $n = p^m$ ,  $p$  prime, the orbit of the subgroup generated by  $T^{p^{m-1}}$  and its conjugate form a complete block system of  $Aut(\mathcal{C})$ );*

*or*

(ii)  $\text{Aut}(\mathcal{C})$  is a doubly-transitive group such that

$$\text{PGL}(d, r^a) \leq \text{Aut}(\mathcal{C}) \leq \text{P}\Gamma\text{L}(d, r^a), \text{ with } n = \frac{r^{ad} - 1}{r^a - 1} \text{ and } a \geq 1.$$

**Proof.** The group  $\text{Aut}(\mathcal{C})$  contains a complete cycle and has composite degree. Hence from a theorem of Burnside and Schur [38, p. 65],  $\text{Aut}(\mathcal{C})$  is either imprimitive or doubly-transitive. If it is imprimitive and  $n = p^m$ , by [12, Ch. XVI Theorem VIII]  $\text{Aut}(\mathcal{C})$  contains an intransitive normal subgroup generated by  $T^{p^{m-1}}$  and its conjugates. By [38, Proposition 7.1] the orbit of such a subgroup forms a complete block system of  $\text{Aut}(\mathcal{C})$ .

In the doubly-transitive case, we have from Lemma 2.2 that the only cases when the socle can be abelian are  $N = C_p$  and  $N = C_2 \times C_2$ . In these cases,  $\text{Aut}(\mathcal{C})$  must be equal to  $\text{AGL}(1, p)$  or  $S_4$ , which is impossible. Since the socle is not abelian and the degree is not prime, this leads to the only solution given by row six of Table 1.  $\square$

**Corollary 2.5** ([32, Corollary 8.6]) *For any circulant graph  $\mathcal{C}$  on  $n$  elements, one of the following holds:*

1.  $\text{Aut}(\mathcal{C}) = S_n$ ;
2.  $\text{Aut}(\mathcal{C})$  is imprimitive, and the orbit of the subgroup generated by  $T^{p^{m-1}}$  and its conjugate form a complete block system of  $\text{Aut}(\mathcal{C})$ ; or
3.  $n$  is prime and  $\text{Aut}(\mathcal{C}) < \text{AGL}(1, p)$ .

**Proof.** If an automorphism group acting on a graph is doubly transitive, then it takes any ordered pair of vertices to another ordered pair of vertices. Hence the graph is either complete or empty, and (in either case) the automorphism group is  $S_n$ . The result then follows from Theorems 2.3 and 2.4.  $\square$

### 3 Automorphism Groups of Cyclic Codes

A linear code  $C$  over  $\mathbb{F}_q$  is cyclic if  $T \in \text{Aut}(\mathcal{C})$ , where  $T = (1, 2, \dots, n)$  is a complete cycle of length  $n$ . In the case of cyclic codes we have the following results concerning the group  $\text{Aut}(\mathcal{C})$ . We begin with the following useful remark.

**Remark 3.1** *The zero code, the entire space, and the repetition code and its dual are called elementary codes. The permutation group of these codes is  $S_n$  [24, p. 1410]. Furthermore, it was proven in [24, p. 1410] that there is no cyclic code with permutation group equal to  $\text{Alt}(n)$ .*  $\square$

The following lemma can be proved using arguments similar to those for the binary case [9, Theorem E Part 3].

**Lemma 3.2** *Let  $\mathcal{C}$  be a non-elementary cyclic code of length  $n = \frac{t^d-1}{t-1}$  over a finite field  $\mathbb{F}_q$ , where  $q = r^\alpha$  and  $t$  is a prime power. If  $\text{Aut}(\mathcal{C})$  satisfies*

$$PGL(d, t) \leq \text{Aut}(\mathcal{C}) \leq P\Gamma L(d, t),$$

*then  $t = r^a$  for some  $a \geq 1$ ,  $d \geq 3$ , and  $\text{Aut}(\mathcal{C}) = P\Gamma L(d, t)$ .*

**Proof.** Assume  $d = 2$ . As the group  $PGL(2, t)$  acts 3-transitively on the 1-dimensional projective space  $\mathbb{P}^1(\mathbb{F}_t)$ , we deduce from [33, Table 1 and Lemma 2] that the underlying code is elementary, which is a contradiction. Hence  $d \geq 3$ , and from [33, Table 1 and Lemma 2], it must be that since  $\mathcal{C}$  is non-elementary,  $t$  must be equal to  $r^a$ . Now let  $V$  denote the permutation module over  $\mathbb{F}_p$  associated with the natural action of  $PGL(d, t)$  on the  $(d-1)$  dimensional projective space  $\mathbb{P}^{d-1}(\mathbb{F}_t)$ . Let  $U_1$  be a  $PGL(d, t)$ -submodule of  $V$ . Hence  $U_1$  is  $P\Gamma L(d, t)$ -invariant. This is because, if  $\sigma$  is a generator of the cyclic group  $P\Gamma L(d, t)/PGL(d, t) \simeq \text{Gal}(\mathbb{F}_t/\mathbb{F}_p)$ , then  $U_2 = U_1^\sigma$ , regarded as a  $PGL(d, t)$ -module, is simply a twist of  $U_1$ . Let  $\overline{\mathbb{F}}_r$  be the algebraic closure of  $\mathbb{F}_r$ . Then the composition factors of the  $\overline{\mathbb{F}}_p PGL(d, t)$ -modules  $\overline{U}_1 = \overline{\mathbb{F}}_r \otimes U_1$  and  $\overline{U}_2 = \overline{\mathbb{F}}_r \otimes U_2$  are the same. The submodules of the  $\overline{\mathbb{F}}_r PGL(d, t)$ -module  $\overline{V} = \overline{\mathbb{F}}_r \otimes V$  are uniquely determined by their composition factors [3]. Then we have  $\overline{U}_1 = \overline{U}_2$ , which implies that  $U_1 = U_2$ , and therefore  $\text{Aut}(\mathcal{C}) = P\Gamma L(d, t)$ .  $\square$

**Theorem 3.3** *Let  $\mathcal{C}$  be a non-elementary cyclic code of length  $n$  over  $\mathbb{F}_q$ , where  $q = r^\alpha$ ,  $\alpha \geq 1$ . Then if  $n = p$  is a prime number we have that  $\text{Aut}(\mathcal{C})$  is a primitive group, and one of the following holds:*

- (i)  *$\text{Aut}(\mathcal{C})$  is a solvable group of order  $pm$  with  $m$  a divisor of  $p-1$  and  $C_p \leq \text{Aut}(\mathcal{C}) \leq \text{AGL}(1, p)$ , with  $p \geq 5$ . Furthermore  $\text{Aut}(\mathcal{C})$  contains a normal  $p$ -Sylow group.*
- (ii) *If  $p = q$ , then  $\text{Aut}(\mathcal{C}) = \text{AGL}(1, p)$ .*
- (iii)  *$\text{Aut}(\mathcal{C}) = \text{PSL}(2, 11)$  and  $q$  is a power of 3.  $\mathcal{C}$  is either an  $[11, 6]$  or  $[11, 5]$  code that is equivalent to the  $[11, 6, 5]$  ternary Golay code or its dual, respectively.*
- (iv)  *$\text{Aut}(\mathcal{C}) = M_{23}$  and  $q$  is a power of 2.  $\mathcal{C}$  is either a  $[23, 12]$  or  $[23, 11]$  code that is equivalent to the  $[23, 12, 7]$  binary Golay code or its dual, respectively.*
- (v)  *$\text{Aut}(\mathcal{C}) = P\Gamma L(d, r^{d^b})$  where  $b \in \mathbb{N}$ ,  $d \geq 3$  is a prime number such that  $(d, r^{d^b} - 1) = 1$ , and  $p = (r^{d^{b+1}} - 1)/(r^{d^b} - 1)$ .*

*If  $n$  is a composite number then  $\text{Aut}(\mathcal{C})$  is either*

(vi) an imprimitive group (in the case that  $n = p^m$ ,  $p$  a prime, the orbit of the subgroup generated by  $T^{p^{m-1}}$  and its conjugate form a complete block system of  $\text{Aut}(\mathcal{C})$ );

or

(vii)  $\text{Aut}(\mathcal{C})$  is a doubly-transitive group equal to  $P\Gamma L(d, r^a)$ , with  $n = \frac{r^{ad}-1}{r^a-1}$  and  $a \geq 1$ .

**Proof.** From Theorem 2.3 we have that  $\text{Aut}(\mathcal{C})$  is either a subgroup of  $AGL(1, p)$  which is solvable of order  $pm$ ,  $m$  a divisor of  $p-1$ , or a doubly transitive group. For the first case if  $p = 2$  or  $3$ , then  $AGL(1, p) = S_p$ , and  $\mathcal{C}$  is elementary by Remark 3.1. For part (ii), if  $q = p$ , Roth and Seroussi [36] proved that any cyclic code of prime length  $p$  over  $\mathbb{F}_p$  must be an MDS code equivalent to an extended Reed–Solomon code. Berger [5] proved that the permutation group of such codes is the affine group  $AGL(1, p)$ . For parts (iii) and (iv), as  $\mathcal{C}$  is non-elementary of prime length  $p$ , by Lemma 2.2, Remark 3.1 and Lemma 3.2, we have that  $\text{Aut}(\mathcal{C})$  is one of  $M_{11}$  with  $p = 11$ ,  $PSL(2, 11)$  with  $p = 11$ ,  $M_{23}$  with  $p = 23$ , or  $P\Gamma L(d, t)$  of degree  $p = (t^d - 1)/(t - 1)$  and  $t$  a prime power. If  $\text{Aut}(\mathcal{C}) = M_{11}$ , from [33, Table 1, Lemma 2]  $\mathcal{C}$  must be elementary, which is a contradiction. If  $\text{Aut}(\mathcal{C}) = PSL(2, 11)$ , from [33, Table 1, Lemma 2 and (J)]  $q$  must be a power of 3, and there is a unique non-elementary code over  $\mathbb{F}_q$  contained in the dual of the repetition code. The  $[11, 5, 6]$  dual of the ternary Golay code is contained in the repetition code and has permutation group  $PSL(2, 11)$ ; its dual, an  $[11, 6, 5]$  code, intersects the dual of the repetition code in this  $[11, 5, 6]$  code and also has permutation group  $PSL(2, 11)$ . Part (ii) then follows. Part (iii) is obtained in an analogous way from [33, Table 1, Lemma 2 and (I)].  $\square$

Now we give an algorithm to find the automorphism group of specific cyclic codes. Let  $\mathcal{C}$  be a non elementary cyclic code over  $\mathbb{F}_r$  of length  $p$ , different from the binary and ternary Golay codes. Further, assume that there are no integers  $b$  and  $d$  such that  $p = (r^{db+1} - 1)/(r^{db} - 1)$ . Then from Theorem 2.3 and Remark 2.1, we have that  $\mathcal{C} \leq AG(p)$ . Let  $a \in \mathbb{Z}_p^*$  and  $\mu_a$  be the associated multiplier. Hence if  $\mu_a(\mathcal{C}) = \mathcal{C}$  then  $\mu_a \in \text{Aut}(\mathcal{C})$ . From Remark 4.8, for all  $b \in \mathbb{Z}_p$  we also have that  $\tau_{a,b} \in \text{Aut}(\mathcal{C})$ . This suggest the following algorithm to find  $\text{Aut}(\mathcal{C})$ . To summarize, it is assumed that  $\mathcal{C}$  is not elementary,  $p \neq 11$  and  $p \neq 23$ , and there are no integers  $b$  and  $d$  such that  $p = (r^{db+1} - 1)/(r^{db} - 1)$ .

#### Algorithm A:

1. Find  $A = \{a \in \mathbb{Z}_p^* \text{ such that } \mu_a(\mathcal{C}) = \mathcal{C}\}$ .
2. If  $A = \mathbb{Z}_p^*$ , then  $\text{Aut}(\mathcal{C}) = AG(p)$ .
3. Otherwise,  $\text{Aut}(\mathcal{C}) = \{\tau_{a,b}, a \in A, b \in \mathbb{Z}_p\}$ .

In Table 2, we give examples of permutation groups of BCH codes of length  $p$  over  $\mathbb{F}_q$ .  $\text{Aut}(\mathcal{C})$  (respectively  $\text{Aut}(\mathcal{C}_2)$  and  $\text{Aut}(\mathcal{C}_3)$ ), denote the permutation groups of narrow sense ( $b = 1$ )

$q$	$p$	$\delta$	$Aut(C)$	$Aut(C_2)$	$Aut(C_3)$
2	17	2	$C_8 \rtimes C_{17}$	$S_{17}$	$S_{17}$
2	23	3	$M_{23}$	$M_{23}$	$M_{23}$
2	41	2	$C_{20} \rtimes C_{41}$	$C_{20} \rtimes C_{41}$	$C_{20} \rtimes C_{41}$
2	41	3	$C_{20} \rtimes C_{41}$	$S_{41}$	$S_{41}$
2	43	5	$C_{14} \rtimes C_{43}$	$C_{14} \rtimes C_{43}$	$C_{14} \rtimes C_{43}$
2	43	7	$C_{14} \rtimes C_{43}$	$S_{43}$	$S_{43}$
3	13	2	$C_3 \rtimes C_{13}$	$C_3 \rtimes C_{13}$	$C_3 \rtimes C_{13}$
3	13	4	$PGL(3, 3)$	$C_3 \rtimes C_{13}$	$C_3 \rtimes C_{13}$
3	13	5	$C_3 \rtimes C_{13}$	$C_3 \rtimes C_{13}$	$C_3 \rtimes C_{13}$
3	23	3	$C_{11} \rtimes C_{23}$	$C_{11} \rtimes C_{23}$	$C_{11} \rtimes C_{23}$
3	41	5	$C_8 \rtimes C_{41}$	$C_8 \rtimes C_{41}$	$C_8 \rtimes C_{41}$
4	43	9	$C_7 \rtimes C_{43}$	$S_{43}$	$S_{43}$
5	11	5	$C_5 \rtimes C_{11}$	$C_5 \rtimes C_{11}$	$C_5 \rtimes C_{11}$
11	5	3	$C_5$	$C_2 \rtimes C_5$	$C_5$

Table 2: Permutation Groups of some BCH Codes of Length  $p$

BCH codes with designed distance  $\delta$  (respectively BCH codes with designed distance  $\delta$  and  $b = 2$  and  $b = 3$ ).

### 3.1 The Automorphism Groups of Cyclic Codes of Length $p^m$

In the previous section, the automorphism groups of cyclic codes were determined. In this section, we provide additional results on these cyclic combinatorial objects in the case  $n = p^m$ , where  $p$  is an odd prime and  $m \geq 1$ .

**Lemma 3.4** *Let  $q$  be a prime power,  $p$  an odd prime, and  $z$  the largest integer such that  $p^z | (q^t - 1)$ , with  $t$  the order of  $q$  modulo  $p$ . If  $z = 1$  we have*

$$\text{ord}_{p^m}(q) = p^{m-1}t.$$

**Proof.** Let  $t$  be the order of  $q$  modulo  $p$ , and  $u = q^t \equiv 1 \pmod{p}$ . Assume that  $z = 1$ , or equivalently  $u \not\equiv 1 \pmod{p^2}$ . It is well known from elementary number theory [16, p. 87] that  $u \pmod{p^m}$  is an element of order  $p^{m-1}$  in the group  $(\mathbb{Z}_{p^m})^*$  if and only if  $u \not\equiv 1 \pmod{p^2}$ . Hence  $\text{ord}_{p^m}(q) = p^{m-1}t$ .  $\square$

Note that according to Brillhart et al. [11], it is unusual to have  $z > 1$ .



**Proposition 3.5** *Let  $\mathcal{C}$  be a cyclic object on  $p^m$  elements with  $m > 1$ . Hence a  $p$ -Sylow subgroup of  $\text{Aut}(\mathcal{C})$  has order  $p^s$  such that*

$$m \leq s \leq p^{m-1} + p^{m-2} + \dots + 1. \quad (2)$$

*We consider  $\mathcal{C}$  to be a cyclic code of length  $p^m$  over  $\mathbb{F}_q$  with  $q = r^\alpha$  a prime power and  $(q, p) = 1$ . Let  $\mu_q$  be the multiplier defined by  $\mu_q(i) = iq \bmod p^m$ . Then the group  $\text{Aut}(\mathcal{C})$  contains the subgroup  $K = \langle T, \mu_q \rangle$  of order  $p^m \text{ord}_{p^m}(q)$ . Let  $p^l$ ,  $l \geq m$ , be the  $p$ -part of the order of  $K$ . Then a  $p$ -Sylow subgroup  $P$  of  $\text{Aut}(\mathcal{C})$  has order  $p^s$  such that*

$$l \leq s \leq p^{m-1} + p^{m-2} + \dots + 1.$$

*If  $z = 1$ , then  $s \geq 2m - 1$ . If  $s = 2m - 1$ , then  $P$  is a transitive group of  $K$ .*

**Proof.** From the definition of a cyclic code, we have that  $T \in \text{Aut}(\mathcal{C})$ . It is obvious that each cyclotomic class modulo  $n$  over  $\mathbb{F}_q$  is invariant under the permutation  $\mu_q$ . This can be deduced from the fact that the polynomial  $f(x) \in \mathbb{F}_q[x]$  satisfies  $f(x^q) = f(x)^q$ . Thus  $\mu_q \in \text{Aut}(\mathcal{C})$ . The order of  $\mu_q$  is equal to  $|Cl(1)| = \text{ord}_{p^m}(q)$ , and hence  $K = \langle T, \mu_q \rangle$  is a subgroup of  $\text{Aut}(\mathcal{C})$  of order  $p^m \text{ord}_{p^m}(q)$ . Then the order of  $K$  has  $p$ -part  $p^l$  with  $l \leq m$ . Let  $P$  be a  $p$ -Sylow subgroup of  $\text{Aut}(\mathcal{C})$  which contains  $T$  (this can always be assumed since any  $p$  group is contained in a  $p$ -Sylow subgroup). Then  $P$  is a  $p$  group of  $S_{p^m}$ . From Sylow's Theorem,  $P$  is contained in a  $p$ -Sylow subgroup of  $S_{p^m}$ . It is well known that a  $p$ -Sylow subgroup of  $S_{p^m}$  has order  $p^{p^{m-1} + p^{m-2} + \dots + 1}$  [35, Kalužnin's Theorem]. Since  $P$  also contains the subgroup of  $K$  of order  $p^l$ , then  $l \leq s \leq p^{m-1} + p^{m-2} + \dots + 1$ . If  $z = 1$ , then by Lemma 3.4 the order of the group  $K$  is  $\text{ord}_p(q)p^{2m-1}$ . This gives that  $p^{2m-1}$  divides  $|\text{Aut}(\mathcal{C})|$ , so  $\text{Aut}(\mathcal{C})$  contains a  $p$  subgroup of order at least  $p^{2m-1}$ . If  $s = 2m - 1$ , we can assume that  $P \leq K$  because we have  $T \in K$  and  $K \leq \text{Aut}(\mathcal{C})$ . Thus  $P$  is a transitive subgroup of  $K$ .  $\square$

**Theorem 3.6** *Let  $\mathcal{C}$  be a non elementary cyclic code of length  $p^m$  over  $\mathbb{F}_{r^\alpha}$  with  $m \geq 1$ . Then the following holds:*

- (i) *If  $p \nmid \alpha$  and  $p \nmid (d, r^a - 1)$ , then  $\text{Aut}(\mathcal{C}) = \text{P}\Gamma\text{L}(d, r^a)$ ,  $a \geq 1$ ,  $d \geq 3$ , if and only if the  $p$ -Sylow subgroup of  $\text{Aut}(\mathcal{C})$  is of order  $p^m$ .*
- (ii) *If  $p \geq 5$ ,  $\alpha = 1$  and  $r = p$ ,  $m > 1$ , then  $\text{Aut}(\mathcal{C})$  is an imprimitive group which admits a complete system formed by the orbit of the subgroup generated by  $T^{p^{m-1}}$  and its conjugate. It also contains a transitive normal  $p$ -Sylow subgroup of order  $p^s$  with  $m < s \leq p^{m-1} + p^{m-2} + \dots + 1$ .*
- (iii) *If  $z = 1$ ,  $p \nmid \alpha$  and  $p \nmid (d, r^a - 1)$ , then  $\text{Aut}(\mathcal{C})$  is an imprimitive group which contains a transitive normal  $p$ -Sylow subgroup of order  $p^s$ , with  $2m - 1 \leq s \leq p^{m-1} + p^{m-2} + \dots + 1$ . Furthermore,  $\text{Aut}(\mathcal{C})$  admits a complete block system formed by the orbit of the subgroup generated by  $T^{p^{m-1}}$  and its conjugate.*

**Proof.** For part (i), we know that the socle of  $P\Gamma L(d, r^a)$  is the group  $PSL(d, r^a)$  of order  $\frac{r^{ad(d-1)/2}}{(d, r^a-1)} \prod_{i=2}^d (r^{ai} - 1)$ . From a lemma of Zsigmondy [25, Ch. IX, Theorem 8.3], except for the cases  $d = 2, r^a = 2^b - 1$  and  $d = 6, r^a = 2$ , there exists a prime  $q_0$  such that  $q_0$  divides  $r^{ad} - 1$ , but does not divide  $r^{ai} - 1$ , for  $1 \leq i < d$ . From Lemma 3.2, we cannot have  $d = 2$ . The case  $d = 6$  and  $r^a = 2$  does not give a prime power. Hence if  $n = p^m = \frac{r^{ad}-1}{r^a-1}$ , there is a  $q_0$  which divides  $(r^{ad} - 1) = (r^a - 1)p^m$ . Since  $q_0$  does not divide  $r^a - 1$ ,  $q_0$  must divide  $p^m$ , and hence  $q_0 = p$  and  $p^m$  is the  $p$ -part of the order of  $PSL(d, r^a)$ . Also, since  $p \nmid r^a - 1$ , we have that  $p \nmid (d, r^a - 1)$ . Hence if  $(\alpha, p) = 1$ ,  $p^m$  is also in the  $p$ -part of the order of  $P\Gamma L(d, r^a)$ , and the result follows.

Conversely, if  $Aut(\mathcal{C})$  contains a  $p$ -Sylow group  $P$  of order  $p^m$ , we can assume that  $T \in P$ , which gives the equality  $P = \langle T \rangle$ . Assume that in this case  $Aut(\mathcal{C})$  is imprimitive. Then by [19, Theorem 33],  $P$  is normal.  $P$  is then the minimal normal subgroup which is transitive and abelian. From [38, p. 17]  $Aut(\mathcal{C})$  is primitive, which is impossible. Thus if  $P = \langle T \rangle$ , the group  $Aut(\mathcal{C})$  is equal to  $P\Gamma L(d, r^a)$ , which is possible only if  $[P\Gamma L(d, r^a) : PSL(d, r^a)]$  is prime to  $p$ , i.e.,  $(p, \alpha) = 1$  and  $p \nmid (d, r^a - 1)$ .

For part (ii), from Theorem 2.4 if  $Aut(\mathcal{C})$  is primitive, then it is doubly-transitive and equal to  $P\Gamma L(d, r^a)$  with  $n = \frac{r^{ad}-1}{r^a-1}, d \geq 3$  and  $a \geq 1$ . From [19, Lemma 22], if  $Aut(\mathcal{C})$  is doubly-transitive with a non abelian socle, then  $Soc(Aut(\mathcal{C})) = Alt(p^m)$ . Hence from Remark 3.1 the code is elementary. Since  $Aut(\mathcal{C})$  is imprimitive, from part (i) the order of the  $p$ -Sylow group is  $p^s$  with  $s > m$ . The second inequality then follows from Proposition 3.5.

For part (iii), if  $z = 1$  then from Proposition 3.5, the order of a  $p$ -Sylow subgroup of  $Aut(\mathcal{C})$  is at least  $p^{2m-1}$ . If  $Aut(\mathcal{C})$  is doubly transitive, by Theorem 2.4 it is equal to  $P\Gamma L(d, r^a)$  with  $d \geq 3$ . By assuming  $p \nmid \alpha$  and  $p \nmid (d, r^a - 1)$ , we obtain from part (i) that a  $p$ -Sylow group of  $Aut(\mathcal{C})$  has order  $p^m$ , which is impossible. Hence  $Aut(\mathcal{C})$  is an imprimitive group. From [19, Theorem 33],  $Aut(\mathcal{C})$  contains a transitive normal  $p$ -Sylow subgroup. The result then follows.  $\square$

**Example 3.7** *The narrow sense BCH code of length 25 over  $\mathbb{F}_3$  with designed distance 3 has an automorphism group which is the imprimitive group  $S_5 \wr S_5$ . The narrow sense BCH code of length 9 over  $\mathbb{F}_5$  with designed distance 2 has an automorphism group which is the imprimitive group  $S_3 \wr S_3$ . The binary  $[7, 4, 3]$  Hamming code has automorphism group  $P\Gamma L(3, 2)$ , which contains a 7-Sylow subgroup of order 7.*

## 4 Equivalence of Cyclic Combinatorial Objects on $p^m$ Elements

Let  $\mathcal{C}$  be a cyclic object of length  $p^m$  where  $p$  is an odd prime,  $m > 1$  and  $P$  is a  $p$ -Sylow subgroup of  $\text{Aut}(\mathcal{C})$ . The following subset of  $S_{p^m}$  was introduced by Brand [10]

$$H(P) = \{\sigma \in S_{p^m} \mid \sigma^{-1}T\sigma \in P\}.$$

The set  $H(P)$  is well defined since  $\langle T \rangle$  is a subgroup of  $\text{Aut}(\mathcal{C})$  of order  $p^m$ , hence it is a  $p$ -group of  $\text{Aut}(\mathcal{C})$ . From Sylow's Theorem, there exists a  $p$ -Sylow subgroup  $P$  of  $\text{Aut}(\mathcal{C})$  such that  $\langle T \rangle \leq P$ . Furthermore, in some cases the set  $H(P)$  is a group.

**Lemma 4.1** (*[10, Lemma 3.1]*) *Let  $\mathcal{C}$  and  $\mathcal{C}'$  be cyclic objects on  $p^m$  elements. Let  $P$  be a  $p$ -Sylow subgroup of  $\text{Aut}(\mathcal{C})$  which contains  $T$ . Then  $\mathcal{C}$  and  $\mathcal{C}'$  are equivalent if and only if  $\mathcal{C}$  and  $\mathcal{C}'$  are equivalent by an element of  $H(P)$ .*

Let  $p$  be an odd prime. For  $n < p$ , we define the following subsets of  $S_{p^m}$ :

$$Q^n = \{f : \mathbb{Z}_{p^m} \rightarrow \mathbb{Z}_{p^m} \mid f(x) = \sum_{i=0}^n a_i x^i, a_i \in \mathbb{Z}_{p^m} \text{ for each } i, (p, a_1) = 1, \\ \text{and } p^{m-1} \text{ divides } a_i \text{ for } i = 2, 3, \dots, n\}.$$

$$Q_1^n = \{f \in Q^n \mid f(x) = \sum_{i=0}^n a_i x^i, \text{ with } a_1 \equiv 1 \pmod{p^{m-1}}\}.$$

The sets  $Q^n$  and  $Q_1^n$  are subgroups of  $S_{p^m}$  [10, Lemma 2.1]. Note that  $Q^1 = AG(p^m)$ .

**Lemma 4.2** *Let  $\mathcal{C}$  be a cyclic object on  $p^m$  elements, where  $p$  is odd and  $m > 1$ . Let  $P$  be a Sylow subgroup of  $\text{Aut}(\mathcal{C})$  which contains  $T$ . If  $1 \leq n < p$ , then*

- (i)  $|Q^n| = (p-1)p^{2m+n-2}$  and  $|Q_1^n| = p^{m+n}$ .
- (ii)  $AG(p^m) = N_{S_{p^m}}(\langle T \rangle) \subset H(P)$ .
- (iii)  $Q^{n+1} = H(Q_1^n)$ .
- (iv)  $N_{S_{p^m}}(Q_1^n) = Q^{n+1}$ .

**Proof.** For part (i), from [10, Lemma 3.2] we have the map  $(a_0, \dots, a_n) \rightarrow f$  where  $f(x) = \sum_{i=0}^n a_i x^i$  is injective if  $n < p-1$ . Thus in  $Q^n$ , the coefficients of  $a_0$  can take  $p^m$  different values, and  $a_1$  can take  $p^{m-1}(p-1)$  values. For  $2 \leq i \leq n$ ,  $a_i$  can take  $p$  values. From these results we have  $|Q^n| = p^{2m+n-2}(p-1)$ . For  $Q_1^n$ , the coefficients of  $a_0$  can take  $p^m$  different values, and  $a_i$  for  $1 \leq i \leq n$  can take  $p$  values, hence  $|Q_1^n| = p^{m+n}$ .

Now we prove that  $AG(p^m) = N_{S_{p^m}}(< T >)$ . Let  $\sigma$  be an element of  $N_{S_{p^m}}(< T >)$ . Then there is a  $j \in \mathbb{Z}_n \setminus \{0\}$  such that  $\sigma T \sigma^{-1} = T^j$ , or equivalently  $\sigma T = T^j \sigma$ . Hence  $\sigma T(0) = \sigma(1) = T^j \sigma(0) = \sigma(0) + j$  and  $\sigma T(1) = \sigma(1) + j = \sigma(0) + 2j$ , so that  $\sigma(k) = \sigma(0) + kj$  for any  $k \in \mathbb{Z}_n$ . Then  $(j, n) = 1$  follows from the fact that the order of  $T$  equals the order of  $T^j$ . The last inclusion is obvious.

Part (iii) follows from [10, Lemma 3.7].

For the proof of part (iv), we begin with the  $\leq$  condition. Let  $h \in N_{p^m}(Q_1^n)$  and  $g = h^{-1}Th$ . As  $T \in Q_1^n$ , it must be that  $g \in Q_1^n$ . Since the order of  $g$  is equal to the order of  $T$  which is  $p^m$ , from [10, Lemma 3.6] there exists  $f \in Q^{n+1}$  such that  $f^{-1}gf = T$ . Thus  $f^{-1}h^{-1}Thf = T$ . The only elements of  $S_{p^m}$  which commute with  $T$  (a complete cycle of length  $p^m$ ), are the powers of  $T$ . Thus  $hf = T^j$  for some  $j$ . Since  $Q^{n+1}$  is a subgroup of  $S_{p^m}$  and  $\langle T \rangle \leq Q^{n+1}$ , then  $h \in Q^{n+1}$ , and hence  $N_{p^m}(Q_1^n) \leq Q^{n+1}$ .

Now consider the  $\geq$  condition. Let  $h \in Q_1^n$ , where  $h(x) = \sum_{i=0}^n h_i x^i$  with  $h_1 \equiv 1 \pmod{p^{m-1}}$  and  $p^{m-1} | h_i$  for  $2 \leq i \leq n$ . Let  $g \in Q^{n+1}$  where  $g(x) = \sum_{i=0}^{n+1} g_i x^i$  with  $p \nmid g_1$  and  $p^{m-1} | g_i$  for  $2 \leq i \leq n$ . We have

$$hg(x) = \sum_{i=0}^n h_i \left( \sum_{j=0}^{n+1} g_j x^j \right)^i = h_0 + h_1 \sum_{i=0}^{n+1} g_j x^j + \sum_{i=2}^n h_i \left( \sum_{j=0}^{n+1} g_j x^j \right)^i.$$

Since  $p^{m-1} | h_i$ , for  $i \geq 2$  and  $p^{m-1} | g_j$  for  $j \geq 2$ , any terms in  $\sum_{i=2}^n h_i \left( \sum_{j=0}^{n+1} g_j x^j \right)^i$  involving  $g_j$  for  $j \geq 2$  vanish modulo  $p^m$ , so that

$$hg(x) = h_0 + h_1 \sum_{j=0}^{n+1} g_j x^j + \sum_{i=2}^n h_i (g_0 + g_1 x)^i.$$

By [10, Lemma 2.1]

$$g^{-1}(x) = \sum_{i=1}^{n+1} b_i x^i, \text{ with } b_1 = g_1^{-1} \text{ and } b_i = -g_i g_1^{-(i+1)} \text{ for } 2 \leq i \leq n+1. \quad (3)$$

We now determine  $g^{-1}hg$  in order to prove that it is in  $Q_1^n$ . This is given by

$$\begin{aligned} g^{-1}hg(x) &= \sum_{k=1}^{n+1} b_k \left( h_0 + h_1 \sum_{j=0}^{n+1} g_j x^j + \sum_{i=2}^n h_i (g_0 + g_1 x)^i - g_0 \right)^k \\ &= b_1 \left( h_0 + h_1 \sum_{j=0}^{n+1} g_j x^j + \sum_{i=2}^n h_i (g_0 + g_1 x)^i - g_0 \right) \\ &\quad + \sum_{k=2}^{n+1} b_k \left( h_0 + h_1 \sum_{j=0}^{n+1} g_j x^j + \sum_{i=2}^n h_i (g_0 + g_1 x)^i - g_0 \right)^k. \end{aligned}$$

As  $p^{m-1}|g_j$  for  $j \geq 2$ , hence  $p^{m-1}|b_k$  for  $k \geq 2$ . Furthermore, we have  $p^{m-1}|h_i$  for  $i \geq 2$ , and thus

$$g^{-1}hg(x) = b_1 \left( h_0 + h_1 \sum_{j=0}^{n+1} g_j x^j + \sum_{j=0}^{n+1} h_i (g_0 + g_1 x)^i - g_0 \right) + \sum_{k=2}^{n+1} b_k (h_0 + h_1 (g_0 + g_1 x) - g_0)^k.$$

Let  $g^{-1}hg(x) = \sum_{m=0}^{n+1} c_m x^m$ , and note that  $c_{n+1} = b_1 h_1 g_{n+1} + b_{n+1} (h_1 g_1) n + 1$ . Then replacing the  $b_i$  with their values from (3), we obtain

$$c_{n+1} = g_1^{-1} h_1 g_{n+1} - g_{n+1} g_1^{-(n+2)} h_1^{n+1} g_1^{n+1} = g_1^{-1} h_1 (g_{n+1} - g_{n+1} h_1^n).$$

As  $h_1 \equiv 1 \pmod{p^{m-1}}$ , we have that  $h_1^n \equiv 1 \pmod{p^{m-1}}$ . In addition, as  $p^{m-1}|g_{n+1}$ , it must be that  $g_{n+1} h_1^n \equiv g_{n+1} \pmod{p^m}$ . Therefore,  $c_{n+1} = 0$ , and  $p^{m-1}|c_i$  for  $2 \leq i \leq n$ . Then we only need to show that  $c_1 \equiv 1 \pmod{p^{m-1}}$ . As  $g_j \equiv 0 \pmod{p^{m-1}}$  for  $j \geq 2$ ,  $h_i \equiv 0 \pmod{p^{m-1}}$  for  $i \geq 2$ , and  $b_k \equiv 0 \pmod{p^{m-1}}$  for  $k \geq 2$ , then  $c_1 \equiv b_1 h_1 g_1 \pmod{p^{m-1}}$ . Finally, since  $b_1 = g_1^{-1}$ , we have that  $c_1 \equiv h_1 \equiv 1 \pmod{p^{m-1}}$ .  $\square$

**Lemma 4.3** *Let  $1 \leq n < p - 1$ . If  $P$  is a  $p$  group of  $S_{p^m}$  with  $Q_1^n \lneq P \leq Q^{n+1}$ , then  $P = Q_1^{n+1}$ .*

**Proof.** By part (ii) of Lemma 4.2, we have  $Q_1^n \triangleleft Q^{n+1}$ . Hence we can consider  $\overline{Q} = Q^{n+1}/Q_1^n$ , which has order  $p^{m-1}(p-1)$  by Lemma 4.2. Let  $N$  be the number of  $p$ -Sylow subgroups of  $\overline{Q}$ . Then by Sylow's Theorem,  $N \equiv 1 \pmod{p}$  and  $N$  divides  $p^{m-1}(p-1)$ . Hence  $N = 1$ , so there exists a unique  $p$ -Sylow subgroup  $\overline{P'}$  of  $\overline{Q}$  which is normal. From the condition on  $P$  above, the image  $\overline{P}$  of  $P$  in  $\overline{Q}$  is also a  $p$ -Sylow subgroup of  $\overline{Q}$ . Since there is a unique  $p$ -Sylow subgroup  $\overline{P'} = \overline{P}$ , by Lemma 4.2 the image  $\overline{Q_1^{n+1}}$  of  $Q_1^{n+1}$  in  $\overline{Q}$  is a  $p$ -Sylow subgroup of  $\overline{Q}$ . Hence  $\overline{Q_1^{n+1}} = \overline{P} = \overline{P'}$ . As  $Q_1^n \lneq P$  and  $Q_1^n \leq Q_1^{n+1}$ , the result follows.  $\square$

Now we prove that the group  $Q_1^1$  is a special subgroup of  $S_{p^m}$ .

**Theorem 4.4** *The group  $Q_1^1$  is a normal subgroup of  $Q^1$  and is the unique subgroup of  $S_{p^m}$  of order  $p^{m+1}$  which contains  $T$ .*

**Proof.** It is obvious that  $T \in Q_1^1$ , and from Lemma 4.2,  $|Q_1^1| = p^{m+1}$ . Consider now an element  $g$  of  $Q^1$ ,  $g(x) = b_0 + b_1 x$ , with  $b_0, b_1 \in \mathbb{Z}_{p^m}$  and  $(b_1, p) = 1$ . It is not difficult to determine that the inverse of  $g$  in  $Q^1$  is given by  $g^{-1}(x) = -b_1^{-1} b_0 + b_1^{-1} x$ . Consider  $f \in Q_1^1$ , so that  $f(x) = a_0 + a_1 x$  with  $a_0, a_1 \in \mathbb{Z}_{p^m}$ ,  $(a_1, p) = 1$  and  $a_1 \equiv 1 \pmod{p^m}$ . We then have  $g^{-1}fg(x) = g^{-1}(a_0 + a_1(b_0 + b_1 x)) = (-b_0 + a_0 + a_1 b_0) b_1^{-1} + a_1 x$ . This proves that  $g^{-1}fg(x) \in Q_1^1$ . Hence  $Q_1^1$  is normal in  $Q^1$ . Now let  $S$  be a subgroup of  $Q^1$  of order  $p^{m+1}$  which contains  $T$ . Thus  $\langle T \rangle$  has index  $p$  in  $S$ , and so  $\langle T \rangle$  is maximal in  $S$ . Furthermore,  $\langle T \rangle \triangleleft S$ , because any subgroup of a  $p$ -group of index  $p$  must be normal. Therefore, we

have  $S = N_S(T) \leq N_{S_{p^m}}(T)$ , and by Lemma 4.2,  $S \leq N_{S_{p^m}}(T) = AG(p^m) = Q^1$ . Thus, such an  $S$  must be a subgroup of  $Q^1$ . It is clear that  $Q^1$  is not abelian, and  $S$  cannot be abelian since it is a transitive group. If this were the case it would have to be a regular group [35, Theorem 1.6.3], and thus  $|S| = p^m$ , which is impossible. Furthermore, the  $p$  groups which contain a cyclic maximal subgroup are known [35, Theorem 5.3.4]. If these groups are not abelian or  $p \neq 2$ , they have the following special forms

$$Q^1_1 = \langle x, T \mid x^p = 1; x^{-1}Tx = T^{1+p^{m-1}} \rangle,$$

and

$$S = \langle y, T \mid y^p = 1; y^{-1}Ty = T^{1+p^{m-1}} \rangle.$$

However, the conditions on  $x$  and  $y$  give that

$$x^{-1}Tx = y^{-1}Ty \iff Tyx^{-1} = yx^{-1}T,$$

so the only elements of  $S_{p^m}$  which commute with  $T$  (a complete cycle of length  $p^m$ ), are the powers of  $T$ . Thus  $yx^{-1} = T^j$  for some  $j$ . Since the order of  $yx^{-1}$  is  $p$ , the only choices for  $j$  are  $j = p^m$  or  $j = p^{m-1}$ . For both choices we get  $S = Q^1_1$ , namely  $j = p^m$  gives that  $x = y^{-1}$  (so  $S = Q^1_1$ ), and  $j = p^{m-1}$  gives that  $x = T^{-p^{m-1}}y$ . Thus we have  $x \in \langle y, T \rangle$ , so that  $\langle x, T \rangle = \langle y, T \rangle$ , and hence  $S = Q^1_1$ .  $\square$

**Theorem 4.5** *Let  $G$  be a subgroup of  $S_{p^m}$  and  $P$  a  $p$ -Sylow subgroup of  $G$  of order  $p^s$  such that  $T \in P$ . Then the following holds:*

- (a) *If  $s = m$ ,  $P = \langle T \rangle$ .*
- (b) *If  $m < s \leq p + m - 1$ , then we have  $P = Q^{s-m}_1$ .*

**Proof.** From Lemma 3.5 we have that  $m \leq s \leq p^{m-1} + p^{m-2} + \dots + 1$ . For the case  $m = s$ , it is obvious that  $P = \langle T \rangle$ . Now, let  $s$  be such that  $m < s \leq p + m - 1$ . Hence  $P$  contains a  $p$ -subgroup  $P'$  of order  $p^{m+1}$ . By Theorem 4.4,  $P' = Q^1_1$ . Let  $j \geq 1$  be the largest integer such that  $Q^j_1 \leq P$ . If  $j = p - 1$ , by Lemma 4.2 we have that  $|Q^{p-1}_1| = p^{p+m-1}$ . Hence the assumption  $s \leq p + m - 1$  leads to the unique solution  $P = Q^{p-1}_1$ . Thus, assume that  $1 \leq j < p - 1$ . If  $Q^j_1 \neq P$ ,  $N_P(Q^j_1)$  properly contains  $Q^j_1$  and by Lemma 4.2,  $N_P(Q^j_1) \leq Q^{j+1}_1$ . As  $Q^j_1 \leq N_P(Q^j_1) \leq Q^{j+1}_1$  and  $Q^j_1 \neq N_P(Q^j_1)$ , by Lemma 4.3  $N_P(Q^j_1) = Q^{j+1}_1$ , a contradiction of the choice of  $j$ .  $\square$

**Theorem 4.6** *Let  $p$  be an odd prime,  $q = r^\alpha$  a prime power,  $C$  a cyclic code over  $\mathbb{F}_q$  of length  $p^m$ ,  $m > 1$  and  $P$  a  $p$ -Sylow subgroup of  $\text{Aut}(C)$  of order  $p^s$  such that  $T \in P$ . Then the following holds:*

- (a) If  $p \nmid \alpha$  and  $p \nmid (d, r^a - 1)$ , then  $s = m$ , and  $P = \langle T \rangle$  if and only if  $\text{Aut}(\mathcal{C}) = \text{P}\Gamma\text{L}(d, r^a)$ ,  $d \geq 3$ .
- (b) If  $p \geq 5$ ,  $\alpha = 1$  and  $r = p$ ,  $m > 1$ , then  $\text{Aut}(\mathcal{C})$  is an imprimitive group and  $P$  is normal of order  $p^s$ ,  $s > m$ . If  $m < s \leq p + m - 1$ , then we have  $P = Q_1^{s-m}$ .
- (c) If  $z = 1$ ,  $p \nmid \alpha$  and  $p \nmid (d, r^a - 1)$ , then  $\text{Aut}(\mathcal{C})$  is an imprimitive group and  $P$  is normal of order  $p^s \geq p^{2m-1}$ . Furthermore, if  $2m - 1 < s \leq p + m - 1$ , then we have  $P = Q_1^{s-m}$ .

**Proof.** Statement (a) and the first parts of (b) and (c) follow from Theorem 3.6. We need only prove that if  $s \leq p + m - 1$ , then  $P = Q_1^{s-m}$ . Assume  $s \leq p + m - 1$ , so that  $P$  contains a  $p$  subgroup  $P'$  of order  $p^{m+1}$ . By Theorem 4.4, we obtain  $P' = Q_1^1$ . Let  $j \geq 1$  be the largest integer such that  $Q_1^j \leq P$ . If  $j = p - 1$ , by Lemma 4.2 we have that  $|Q_1^{p-1}| = p^{p+m-1}$ . Thus  $Q_1^{p-1}$  is a subgroup of  $P$  of the same order as  $P$ , and hence  $P = Q_1^{p-1}$ , so we can assume that  $1 \leq j < p - 1$ . If  $Q_1^j \subsetneq P$ , then  $Q_1^j \subsetneq N_P(Q_1^j)$  and by Lemma 4.2,  $N_P(Q_1^j) \leq Q_1^{j+1}$ . Since  $Q_1^j \subsetneq N_P(Q_1^j) \leq Q_1^{j+1}$ , by Lemma 4.2  $N_P(Q_1^j) = Q_1^{j+1}$ , which contradicts the choice of  $j$ .  $\square$

**Corollary 4.7** *Let  $\mathcal{C}$  and  $\mathcal{C}'$  be two cyclic combinatorial objects on  $p^m$  elements, and let  $P$  be a  $p$ -Sylow subgroup of  $\mathcal{C}$  such that  $T \in P$ . If  $|P| = p^s$  and  $s \leq p + m - 1$ , then  $\mathcal{C}$  and  $\mathcal{C}'$  can be equivalent only under the permutation of the following subgroups of  $S_{p^m}$ :*

- (i)  $\text{AG}(p^m)$  if  $s = m$ ;
- (ii)  $Q^{s-m+1}$  if  $s > m$ .

**Proof.** The result follows from Lemma 4.1, Theorem 4.6 and Lemma 4.2.  $\square$

**Remark 4.8** *Since each affine transformation can be written as the product of a power of  $T$  and a multiplier, and since  $T \in \text{Aut}(\mathcal{C})$  the power of  $T$  is absorbed in  $\text{Aut}(\mathcal{C})$ . Hence the permutation given in part (i) of Corollary 4.7 is reduced to a multiplier.*

In order to solve the isomorphism problem for cyclic combinatorial objects, we must know the  $p$ -Sylow subgroup of  $\text{Aut}(\mathcal{C})$ . To determine this, consider the following polynomial permutations  $f_1 = T$  and  $f_i(x) = 1 + x + p^{m-1}(x^2 + \dots + x^i)$  for  $2 \leq i \leq p - 2$ .

**Corollary 4.9** *Let  $G$  be a subgroup of  $S_{p^m}$  with a  $p$ -Sylow subgroup  $P$ , and let  $I$  be the largest value of  $i$  such that  $f_i \in G$ . If  $I < p - 2$ , then we have  $P = Q_1^I$ .*

**Proof.** Assume that  $I$  is the largest  $i$  such that  $f_i \in G$  and  $I < p - 2$ . Let  $P$  be a  $p$ -Sylow subgroup of  $G$  of order  $s$ . Let  $s$  be such that  $I + m \leq s < p + m - 1$ . From Theorem 4.6, we have that a  $p$ -Sylow subgroup of any subgroup of  $G \leq S_{p^m}$  which contains  $T = f_1$  and has order  $p^s$  with  $m \leq s \leq p + m - 1$ . Then we have  $P = T$  when  $s = m$  or  $P = Q_1^{s-m}$ , so in this case  $s - m = I$ . Now, if  $s \leq I + m \leq p + m - 1$ , we have from Theorem 4.6 that  $P = Q_1^{s-m}$ , so  $Q_1^I \cap G \leq Q_1^{s-m}$ . The assumption on  $I$  gives  $I = s - m$ .

Assume now that  $s > p + m - 1$ . Since  $I < p - 2$ , we have that  $s > p + m - 1 > m + I$ . We will prove that this case cannot occur. We have  $T = f_1 \in Q_1^1$ . From Theorem 4.4,  $Q_1^1$  is the unique subgroup of  $S_{p^m}$  of order  $p^{m+1}$  which contains  $T$ . Hence  $Q_1^1 \not\leq P$ . Since  $Q_1^1 \not\leq Q_1^2$ , it must be that  $Q_1^1 \leq Q_1^2 \cap P \leq Q^2$ . Hence from Lemma 4.3 we obtain  $Q_1^2 \cap P = Q_1^2$  which gives  $Q_1^2 \leq P$ . Using the same approach for  $2 \leq i \leq I$ , we obtain  $Q_i \leq P$ . The assumption on  $s$  gives that  $Q_I \leq P$ . Hence  $Q_1^I \leq Q_1^{I+1} \cap P \leq Q^{I+1}$  ( $Q^{I+1}$  can be considered since it was assumed that  $I < p - 2$ ). Hence from Lemma 4.3 we obtain  $Q_1^{I+1} \cap P = Q_1^{I+1}$ . This contradicts the assumption on  $I$ .  $\square$

This corollary suggest the following algorithm for  $I < p - 2$ .

**Algorithm B:** Let  $p$  be an odd prime, and  $\mathcal{C}$  and  $\mathcal{C}'$  be two cyclic combinatorial objects from the same category. Then the equivalence of  $\mathcal{C}$  and  $\mathcal{C}'$  can be determined as follows.

**Step 1:** Find the order of the Sylow subgroup of  $\text{Aut}(\mathcal{C})$  as follows. Find the largest  $I$  such that  $f_I \in \text{Aut}(\mathcal{C})$ . Then  $s = i + m$ , and do Step 2.

**Step 2,** find  $f \in Q^{I+1}$  such that  $\mathcal{C}' = f\mathcal{C}$ .

**Remark 4.10** To find the required  $I$  in Algorithm B we can use (for example) a binary search which requires checking at most  $\lceil \log_2(p-1) \rceil + 1$  of the  $f_i$ . Furthermore, the cardinality of  $Q^{I+1}$  is  $(p-1)p^{2m+I-2}$ .

**Definition 4.11** The cycle graph on  $n$  vertices is the graph  $\mathcal{C}_n$  with vertex set  $\{0, 1, \dots, n-1\}$  and  $i$  adjacent to  $j$  if and only if  $j - i \equiv \pm 1$ .

**Corollary 4.12** Two cycle graphs  $\mathcal{C}_n$  and  $\mathcal{C}'_n$  on  $p^m$  vertices can be isomorphic only by a multiplier.

**Proof.** The automorphism group of a cycle graph on  $n$  vertices has order  $2n$  [21, Ex. 2 p. 30]. Hence if  $n = p^m$ , there is a unique Sylow subgroup of  $\text{Aut}(\mathcal{C}_n)$  of order  $p^m$ . Then the result follows from Corollary 4.7 and Remark 4.8.  $\square$



## References

- [1] B. Alspach and T. D. Parson, *Isomorphism of circulant graphs and digraphs*, Discr. Math., 25(2), 97–108, 1979.
- [2] L. Babai, P. Codenotti, and J. A. Groshow, *Code equivalence and group isomorphism*, in Proc. ACM-SIAM Symp. on Discr. Algorithms, San Francisco CA, 1395–1408, 2011.
- [3] M. Bardoe and P. Sin, *The permutation modules for  $GL(n + 1, \mathbb{F}_q)$  acting on  $\mathbb{P}^n(\mathbb{F}_q)$  and  $\mathbb{F}_q^{n+1}$* , J. London Math. Soc., 61, 58–80, 2000.
- [4] S. Bays, *Sur les systèmes cycliques de triples de Steiner différents pour  $N$  premier (ou puissance d'un nombre premier) de la forme  $6n + 1$* , I, Comment. Math. Helv., 2, 294–305, 1930.
- [5] T. P. Berger, *A direct proof for the automorphism group of Reed–Solomon codes*, Proc. Eurocode 90, G. Cohen and P. Charpin, Eds., Lecture Notes in Computer Science 514, Springer-Verlag, Berlin, 21–29, 1991.
- [6] T. P. Berger, *On the automorphism groups of affine invariant codes*, Designs, Codes, Crypt., 7, 215–221, 1996.
- [7] T. P. Berger and P. Charpin, *The permutation group of affine invariant extended cyclic codes*, IEEE Trans. Inform. Theory, 62(6), 2194–2209, Nov. 1996.
- [8] A. Benyamini-Seeyar, S. G. S. Shiva, and V. K. Bhargava, *Capability of error trapping technic in decoding cyclic codes*, IEEE Trans. Inform. Theory, 32(2), 166–180, 1986.
- [9] R. Bienert and B. Klopsch, *Automorphism groups of cyclic codes*, J. Algebraic Combin., 31(1), 33–52, 2010.
- [10] N. Brand, *Polynomial isomorphisms of combinatorial objects*, Graphs and Combin., 7(1), 7–14, 1991.
- [11] J. Brillhart, J. Tonascia, and P. Weinberger, *On the Fermat quotient*, in Computers in Number Theory, A. O. L. Atkin and B. Birch, Eds., pp. 213–222, Academic Press, New York, 1991.
- [12] W. Burnside, *On some properties of groups of odd order*, J. London Math. Soc., 33, 162–185, 1901.
- [13] W. Burnside, *Theory of Groups of Finite Order*, Dover, Mineola NY, 1955.
- [14] P. J. Cameron, *Finite permutation group and finite simple groups*, Bull. London Math. Soc., 13, 1–22, 1981.

- [15] H. Cao and R. Wei, *Combinatorial Constructions for Optimal Two-Dimensional Optical Orthogonal Codes*. IEEE Trans. Inform. Theory 55(3): 1387-1394, 2009.
- [16] M. Demazure, *Cours D'Algèbre: Primalité, Divisibilité, Codes*, Cassini, Paris, 1997.
- [17] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics 163, Springer-Verlag, Berlin, 1996.
- [18] J. D. Dixon and A. Zalesskii, Finite primitive linear groups of prime degree, J. London Math. Soc., 57(2), 126–134, 1998.
- [19] E. D. Dobson, *On groups of odd prime-power degree that contain a full cycle*, Discr. Math., 299, 65–78, 2005.
- [20] E. D. Dobson and D. Witte, *Transitive permutation groups of prime-squared degree*, J. Algebraic Combin., 16(1), 43–69, 2002.
- [21] C. Godsil, *Algebraic Graph Theory*, Springer, New York, 2001.
- [22] M. Hall Jr., *The Theory of Groups*, MacMillan, New York, 1970.
- [23] W. C. Huffman, V. Job, and V. Pless, *Multiplier and generalized multipliers of cyclic objects and cyclic codes*, J. Combin. Theory. A, 62, 183–215, 1993.
- [24] W. C. Huffman, *Codes and groups*, in V. S. Pless and W. C. Huffman, Eds., Handbook of Coding Theory, Elsevier, Amsterdam, 1345–1439, 1998.
- [25] B. Huppert and N. Blackburn, *Finite Groups II*, Grundlehren Math. Wiss. 242, Springer-Verlag, Berlin, 1982.
- [26] M. Ch. Klin and R. Pöschel, *The isomorphism problem for circulant graphs and digraphs with  $p^n$  vertices*, Akad. der Wiss. der DDR, ZIMM, Berlin, 1980.
- [27] F. Lim, M. Fossorier, and A. Kavčič, *Notes on the automorphism group of Reed–Solomon binary images*, in Proc. IEEE Int. Symp. Inform. Theory, Toronto, Canada, 1813–1817, July 2008.
- [28] P. Lambossy, *Sur une manière de différencier les fonctions cycliques d'une forme donnée*, Comment. Math. Helv., 3, 69–102, 1931.
- [29] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting-Codes*, North-Holland, Amsterdam, 1977.
- [30] R. J. McEliece, *A Public-Key Cryptosystem Based On Algebraic Coding Theory*, DSN Progress Report 42-44, 114–116, Jan.-Feb. 1978.

- [31] J. P. McSorley, *Cyclic permutation groups in doubly-transitive groups*, Comm. Algebra 25, 33–35, 1997.
- [32] J. Morris, *Automorphism groups of circulant graphs – A survey*, Graph Theory, Trends in Math., Birkhauser, 2006.
- [33] B. Mortimer, *The modular permutation representations of the known doubly transitive groups*, Proc. London Math. Soc., 41, 1–20, 1980.
- [34] M. Muzyschuk, *On the isomorphism problem for cyclic combinatorial objects*, Discr. Math. 197/198, 589–606, 1999.
- [35] D. J. S. Robinson, *A Course in the Theory of Groups*, Graduate Texts in Mathematics 80, Springer-Verlag, Berlin, 1980.
- [36] R. Roth and G. Seroussi, *On cyclic MDS codes of length  $q$  over  $GF(q)$* , IEEE Trans. Inform. Theory, 32(2), 284–285, Mar. 1986.
- [37] M. Walch and G. Gantz, *Pictographic matching: A graph-based approach towards a language independent document exploitation platform*, in Proc. ACM Workshop on Hard-copy Document Process., 53–62, Washington DC, Nov. 2004.
- [38] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.